RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **KEY-W01S**

Global Threat Brief

DMITRI ALPEROVITCH

Co-Founder and former CTO, CrowdStrike
Board Member: Dragos, Scythe
@DAlperovitch


NEW
BEGINNING

RSAConference2020

2019 in Review

Key Trends in 2019

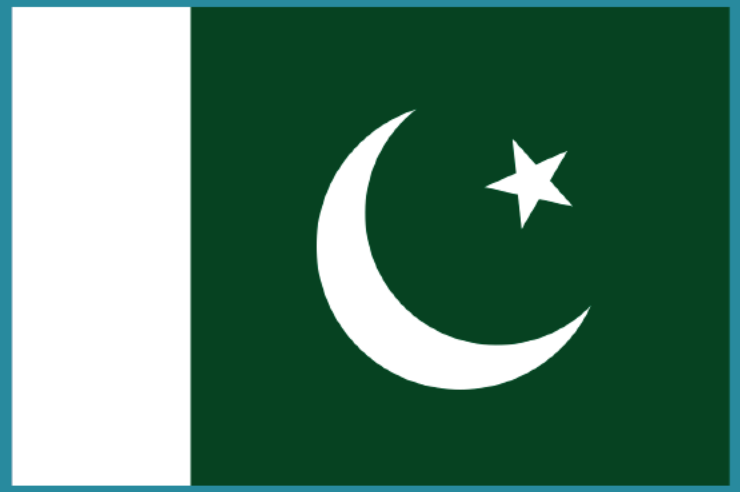
- Ransomware, Ransomware, Ransomware
- It's not all about China and Russia…
- North Korea, Iran, Vietnam, Pakistan are increasing their operational tempo
- Russia stayed low key in 2019
- Chinese MSS operations continue unabated

Ransom Phenomenon

- Everyone is a target
- Top Families: Ryuk, REvil / GandCrab (terminated)
- Ryuk
  - Delivered by Russian-based cybercrime group (Wizard Spider) , often via TrickBot or Emotet trojans
  - Operating since August 2018
  - Recent changes enable Wake-on-LAN and ARP ping scan to maximize number of encrypted systems
  - SMB-based mounting
  - Typical ransom payment can be $100k-$1m
  - Paying ransom may not solve your problems
  - Typical time from infection to encryption: hours to days
- ‘We have backups’

Pakistan: Sneaking under the Radar

- Names: Mythic Leopard, APT 36, Lapis, Op Transparent Tribe
- Karachi, Pakistan-based adversary
- Traditionally targeted India, NATO and UN
- Recently: Western Industry
- Custom RAT



Vietnam: We love IP too

- Names: Ocean Buffalo, APT 32, OceanLotus
- Hanoi, Vietnam-based adversary
- Traditionally targeted China, Cambodia and Vietnam targets
- First foray into IP theft (automotive) in 2018
- Expansion into other sectors in 2019

Iran: Bombs, Drones and Malware

- Names: Charming Kitten, APT35, Newscaster, Parastoo
- Iran-based adversary
- Traditionally focuses on strategic intelligence collection against US and other Middle Eastern governments
- June 13: Limpet mine attack on tankers in the Gulf
- TTPs: Spearphish, Obfuscated powershell, FTP

North Koreans in High Gear

- Names: Velvet Chollima, Kimsuki
  - Intrusions into think tanks and universities
  - TTPs
    - Installation of crypto miners
    - Chrome password stealer and malicious plugins
    - Web vulnerability scanner
    - Quasar and NavRAT implants
- Names: Stardust Chollima, APT38, Bluenoroff
  - Financial institution targeting, including SWIFT
  - TTPs
    - RDP with harvested credentials
- Names: Labyrinth Chollima, Red Dot
  - IP Theft

China: Indictment strategy success?

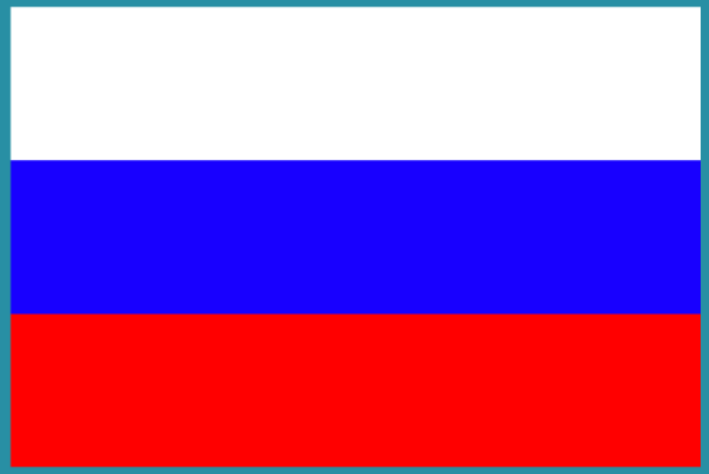
- What happened to PLA?



- Indictments having an effect?
  - Comment Panda AKA APT1, Unit 61398 (May 2014)
  - Gothic Panda AKA APT3, Boyusec (November 2017)
  - Stone Panda AKA APT10, Huaying Haitai (December 2018)
- MSS keeps up high operational tempo
- Insider-assisted operations
- Other actors:
  - Wicked Panda/Spider, APT41, Winnti
  - Emissary Panda, APT27, Bronze Union

Low Key Year for Russia

- Limited operational tempo
- Fancy Bear, APT28
  - Continued spearphishing of strategic political priorities
  - Big focus on Ukraine
- Venomous Bear, Turla, Snake
  - Big focus on Middle East
  - Take over of Iranian C2 Infrastructure (Helix Kitten / APT 34)



What's next?

- Iran: Destructive attacks likely
- Russia: Expected increased activity in 2020
- China: Escalation of espionage campaigns
- IP Theft: Iran, Vietnam, North Korea, Pakistan, India, ?
- US/5Eyes: 'Persistence Engagement' strategy more aggressive
- More indictments/sanctions, collective attribution action
- 'Cyber Peace' not coming anytime soon

RSAConference2020

Conclusions

Our Industry is Full of Contradictions

Threat Model Differences

	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Trusted insiders steal proprietary information for personal, financial, and ideological reasons.	Nation-state actors conduct computer intrusions to steal sensitive state secrets and propriety information from private companies.	Terrorist groups sabotage the computer systems that operate our critical infrastructure, such as the electric grid.	Nation-state actors sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

Always consider the Trade Offs

Other Trends

- Policy is in the next frontier
  - More regulations are coming (Section 230, encryption, data breach laws..)
  - Government action establishes de-facto norms
  - Private Sector is not a neutral party in the fight
- Technology
  - Persistence will be redefined (Browsers, Messaging Apps)
  - K8/Containers are the new OS
  - Source code manipulation to become more prevalent
- Strategy
  - 'The bomber will always get through' , but stealth is hard and dwell time is coming down
  - Deterrence largely ineffective
  - Insider infiltration at large tech companies to become routine
  - Persistent Engagement is not just a USCYBERCOM strategy but today's reality
  - Silver lining: Offense against hard targets is more costly than ever

RSAConference2020

THANK YOU!

@DAlperovitch